Recurring Sequences over Vector Spaces

Surjeet Singh
Department of Mathematics
Kuwait University
P.O. Box 5969
13060 Safat, Kuwait

Submitted by Hans Schneider

ABSTRACT

Let F be a Galois field and k be a fixed p itive integer. The set $\Gamma_k(F)$ of all sequences over $F^{k\times 1}$ is made into a left R-module, where $R = F[D]^{k\times k}$. For any subset X of R, let $\Omega_k(X) = \{S \in \Gamma_k(F): f(D)S = 0 \text{ for all } f(D) \in X\}$. Let $L_k(F)$ be the set of all $\Omega_k(f(D))$, where $f(D)$ runs over regular elements of R. $L_k(F)$ is shown to be closed under finite sums and intersections. For any regular $f(D)$, the periodicity properties of members of $\Omega_k(f(D))$ are studied; a theorem giving a canonical form of $\Omega_k(f(D))$ is established.

INTRODUCTION

Many authors have attempted to develop the theory of linear recurrence sequences over some types of rings or modules. (See [1], [2], [3], [4], [9], [10], [11], and [14.) In most of the cases the structure theory is not as satisfactory as over a Galois field; the reason being that the ring or the module considered is too general or the sequences considered are of special kinds. The structure theory of prime, principal left and right ideal rings is well developed (see [5, 7]). Keeping this in view, we consider the ring $R = F[D]^{k\times k}$, where F is a Galois field. R is a prime, hereditary, principal left and right ideal ring. For $f(D) = \sum_{i=1}^{m} a_i D^i \in R$ and $S = (s_n) \in \Gamma_k(F)$ indexed by integers $n \geq 0$, define $f(D)S = (\omega_n)$, where $\omega_n = \sum_i a_i s_{n+i}$. This makes $\Gamma_k(F)$ into a left R-module. For any regular (i.e., not a zero divisor) $f(D) \in R$, there exists a unique monic polynomial $\lambda(D) \in F[D]$ of smallest degree such that $R\lambda(D)$

655 Avenue of the Americas, New York, NY 10010 0024-3795/90/$3.50

$\subset Rf(D)$, and a unique $f^*(D) \in R$ such that $f(D)f^*(D) = \lambda(D)I_k$. Theorem 2.3 shows that

$$\Omega_k(f(D)) = f^*(D)\Omega_k(\lambda(D)I_k).$$

Theorem 2.6 gives a relationship between the periods of members of $\Omega_k(f(D))$ and that of members of $\Omega_1(\lambda(D))$. Theorem 3.2 gives a canonical form of $\Omega_k(f(D))$. Finally an elementary example is given to illustrate the various concepts discussed in the paper.

1. PRELIMINARIES

We review some results on ring theory, which we need in this paper. Most of these can be found in [5]. A module M is said to be uniserial if the lattice of its submodules is finite and linearly ordered under inclusion. A ring S is said to be generalized uniserial if $S = \oplus \sum_{i=1}^{r} e_i S = \oplus \sum_{i=1}^{r} Se_i$ for some orthogonal indecomposable idempotents e_i, $1 \leqslant i \leqslant r$, such that each of $e_i S$ and Se_i is a uniserial module. A finite direct sum of primary generalized uniserial rings is called a uniserial ring. These rings under different terminology are discussed in Faith [5, Chapter 25]. Any module over a generalized uniserial ring is a direct sum of uniserial modules.

Let F be a Galois field. For a fixed positive integer k, let $R = F[D]^{k\times k} = F^{k\times k}[D]$. For any nonzero ideal $R\lambda(D)$ of R, $R/R\lambda(D)$ is a uniserial ring. For $f(D) = [f_{ij}(D)] \in R$, adj$(f(D))$ and $|f(D)|$ will denote the adjoint and the determinant respectively of $f(D)$. Any $\lambda(D) \in F[D]$ will be identified with $\lambda(D)I_k$, where I_k is the $k \times k$ identity matrix. Let $f(D) \in R$ be regular. Since $f(D)\cdot\text{adj}(f(D)) = |f(D)|I_k$, $f(D)R$ contains a nonzero ideal. So there exists a unique monic polynomial $\lambda(D) \in F[D]$ such that $R\lambda(D)$ is the largest ideal contained in $Rf(D)$; hence also in $f(D)R$. This polynomial $\lambda(D)$ is called the bound of $f(D)$. For any matrix A over any set X, A^T denotes the transpose of A. For any right ideal I of a matrix ring $s^{k\times k}$ over a commutative ring S, the S-submodule of $S^{k\times 1}$ consisting of all the columns of members of I is called the column module of I. Given any S-submodule K of $S^{k\times 1}$, there exists a unique right ideal J of $S^{k\times k}$ whose column module is K; J is precisely the set of those matrices in $S^{k\times k}$ whose columns are in K. We have the following (see [8, p. 136]).

LEMMA 1.1. *Any two right ideals I and I' of $S^{k\times k}$ are equal if and only if they have the same column modules.*

For any module M and any $n \geq 1$, M^n (also $\oplus\Sigma_1^n M$) denotes the direct sum of n copies of M. For general terms in ring theory we refer to Faith [5], and for linear recurrence sequences to [9] and [12].

2. THE LATTICE $L_k(F)$

Throughout, F is a Galois field, and for a fixed positive integer k, $R = F[D]^{k\times k}$. Now $\Gamma_1(F)^{k\times 1}$ is a left R-module such that for $[f_{ij}(D)] \in R$ and $S = [S_1, S_2, \ldots, S_k]^T \in \Gamma_1(F)^{k\times 1}$,

$$[f_{ij}(D)]S = [S_1', S_2', \ldots, S_k']^T,$$

where $S_i' = \Sigma_{j=1}^k f_{ij}(D)S_j$. Similarly $\oplus\Sigma_1^k\Gamma_1(F)$ is a left $R-$module. Since these two modules and $\Gamma_k(F)$ are isomorphic as left R-modules, we shall regard them as the same. We start with the following lemma, which can be easily proved by using elementary properties of matrices.

LEMMA 2.1. *Let $f(D) = [f_{ij}(D)] \in R$ be regular with bound $\lambda(D)$.*

(i) *There exists a unique $f^*(D) \in R$ such that $f(D)f^*(D) = f^*(D)f(D) = \lambda(D)I_k$.*

(ii) *$\lambda(D)$ divides $|f(D)|$.*

(iii) *If $\operatorname{adj}(f(D)) = [g_{ij}(D)]$ and $\mu(D) = \gcd(g_{ij}(D))$, then*

$$f^*(D) = c^{-1}\left[\frac{g_{ij}(D)}{\mu(D)}\right]$$

and $\lambda(D) = c^{-1}\mu(D)^{-1}|f(D)|$, where c is the leading coefficient of $|f(D)|$.

(iv) *For any monic polynomial $\nu(D) \in F[D]$, $\operatorname{bound}(\nu(D)f(D)) = \nu(D)\lambda(D)$ and $(\nu(D)f(D))^* = f^*(D)$.*

(v) *$\{h(D) \in R : f(D)h(D) \in R\lambda(D)\} = f^*(D)R$ and $\{h(D) \in R : h(D)f(D) \in R\lambda(D)\} = Rf^*(D)$.*

(vi) *The bound $\lambda^*(D)$ of $f^*(D)$ is $\lambda(D)/\kappa(D)$, where $\kappa(D) = \gcd(f_{ij}(D))$ and $f^{**}(D) = [f_{ij}(D)/\kappa(D)]$.*

Consider any regular $f(D) = \Sigma_{i=0}^m a_i D^i$, $a_m \neq 0$, in R. Since $a_m \in F^{k\times k}$ need not be invertible, there may exist distinct sequences $S = (s_n)$ and $S' = (s_n')$ in $\Omega_k(f(D))$ with $s_i = s_i'$ for $0 \leq i \leq m-1$. This is unlike the case for $k = 1$. Let $\lambda(D) \in F[D]$ be a monic polynomial of positive degree. For

$A = [S_{ij}] \in \Omega_1(\lambda(D))^{k\times k}$ and $g(D) = [g_{ij}(D)] \in R$, the usual matrix multiplication $g(D)A$ makes $\Omega_1(\lambda(D))^{k\times k}$ a left R-module, and

$$\Omega_1(\lambda(D))^{k\times k} \approx \Omega_k(\lambda(D)I_k)^k.$$

For any $S \in \Omega_1(\lambda(D))$ with $\lambda(D)$ as its minimal polynomial we know that

$$\Omega_1(\lambda(D)) = F[D]S \approx F[D]/F[D]\lambda(D).$$

Here we have the following.

LEMMA 2.2. *Let $\lambda(D)$ be any nonconstant monic polynomial in $F[D]$, and S be any member of $\Omega_1(\lambda(D))$ having $\lambda(D)$ as its minimal polynomial. Then:*

(i) $\sigma: R/R\lambda(D) \to \Omega_1(\lambda(D))^{k\times k}$ *such that for* $g(D) = [g_{ij}(D)] \in R$,

$$\sigma\left(\overline{g(D)}\right) = [g_{ij}(D)S]$$

is a left R-module isomorphism.

(ii) *For any $F[D]$-submodule K of $\Omega_1(\lambda(D))^{k\times 1}$, let J be the set of those matrices in $\Omega_1(\lambda(D))^{k\times k}$ whose columns are in K. Then $\sigma^{-1}(J)$ is a right ideal of $R/R\lambda(D)$ with its column module isomorphic to K.*

Proof. (i) is obvious, and (ii) follows from (i) and Lemma (2.1). ∎

THEOREM 2.3. *Let $f(D) \in R$ be regular with bound $\lambda(D)$. Then*

$$\Omega_k(f(D)) = f^*(D)\Omega_k(\lambda(D)I_k)$$

and

$$\Omega_k(\lambda(D)I_k = R\Omega_k(f(D)).$$

Proof. Since $f^*(D)f(D) = \lambda(D)I_k$, $\Omega_k(f(D)) \subset \Omega_k(\lambda(D)I_k)$. Choose any $S \in \Omega_1(\lambda(D))$ with $\lambda(D)$ as its minimal polynomial; one such S is the impulse response sequence with characteristic polynomial $\lambda(D)$ [9, Corollary 8.52]. Now $\Omega_k(f(D))$ is an $F[D]$-submodule of $\Omega_k(\lambda(D)I_k)$. By Lemma

2.2(ii), $\sigma^{-1}(\Omega_k(f(D))^k)$ is a right ideal of $R/R\lambda(D)$ with its column module isomorphic to $\Omega_k(f(D))$. Any member of $\Omega_1(\lambda(D))^{k\times k}$ is of the form $g(D)(SI_k)$, $g(D)\in R$. Thus $g(D)(SI_k)\in\Omega_k(f(D))^k$ if and only if $f(D)g(D)(SI_k)=0$. By Lemma 2.2(i) it is equivalent to $f(D)g(D)\in R\lambda(D)$. Hence by Lemma 2.1(v)

$$\sigma^{-1}\big(\Omega_k(f(D))^k\big)=f^*(D)R/R\lambda(D).$$

Consequently by applying σ, we get

$$\Omega_k(f(D))=f^*(D)\Omega_k(\lambda(D)I_k).$$

Consider $Rf^*(D)R$. Since by Lemma 2.1(iii) the gcd of entries of $f^*(D)$ is 1, $Rf^*(D)R=R$. Hence

$$\Omega_k(\lambda(D)I_k)=Rf^*(D)R\Omega_k(\lambda(D)I_k)=R\Omega_k(f(D)).$$

This proves the theorem. ∎

PROPOSITION 2.4. *Let $\mu(D)\in F[D]$ be a nonconstant monic polynomial, and $f(D)\in R$ be regular with bound $\lambda(D)$, a factor of $\mu(D)$. Then:*

(i) $\Omega_k(f(D))=f^*(D)\dfrac{\mu(D)}{\lambda(D)}\Omega_k(\mu(D)I_k)$.

(ii) $\Omega_k(f^*(D))=f(D)\Omega_k(\lambda(D)I_k)$.

(iii) $f(D)\Omega_k(\mu(D)I_k)=\Omega_k\left(\dfrac{\mu(D)}{\lambda(D)}f^*(D)\right)$.

(iv) *Any finite $F[D]$-submodule of $\Gamma_k(F)$ is in $L_k(F)$.*

Proof. Let $S\in\Omega_1(\mu(D))$ have $\mu(D)$ as its minimal polynomial. Then $\Omega_1(\mu(D))=F[D]S\approx F[D]/F[D]\mu(D)$ gives

$$\Omega_1(\lambda(D))=\frac{\mu(D)}{\lambda(D)}\Omega_1(\mu(D)),$$

so that

$$\Omega_k(\lambda(D)I_k)=\frac{\mu(D)}{\lambda(D)}\Omega_k(\mu(D)I_k).$$

This fact together with Theorem 2.3 gives (i). Let $\kappa(D)$ be the gcd of entries of $f(D)$. By Lemma 2.1(vi), $f^{**}(D) = [1/\kappa(D)]f(D)$ and $\text{bound}(f^*(D)) = \lambda(D)/k(D)$. So

$$\Omega_k(f^*(D)) = f^{**}(D)\Omega_k\left(\frac{\lambda(D)}{\kappa(D)}I_k\right)$$

$$= \frac{1}{\kappa(D)}f(D)\Omega_k\left(\frac{\lambda(D)}{\kappa(D)}I_k\right)$$

$$= f(D)\Omega_k(\lambda(D)I_k).$$

This proves (ii). Now

$$\text{bound}\left(\frac{\mu(D)}{\lambda(D)}f^*(D)\right) = \frac{\mu(D)}{\kappa(D)} \quad \text{and} \quad \left(\frac{\mu(D)}{\lambda(D)}f^*(D)\right)^* = f^{**}(D).$$

We get

$$\Omega_k\left(\frac{\mu(D)}{\lambda(D)}f^*(D)\right) = f^{**}(D)\Omega_k\left(\frac{\mu(D)}{\kappa(D)}I_k\right)$$

$$= \frac{1}{\kappa(D)}f(D)\Omega_k\left(\frac{\mu(D)}{\kappa(D)}I_k\right)$$

$$= f(D)\Omega_k(\mu(D)I_k).$$

This proves (iii). Finally, let M be a finite $F[D]$-submodule of $\Gamma_k(F)$. We can find a monic polynomial $\mu(D)$ of positive degree in $F[D]$ such that $\mu(D)M = 0$. Consequently $M \subset \Omega_k(\mu(D)I_k)$. By Lemma 2.2(i), $\sigma^{-1}(M^k)$ is a right ideal of $R/R\mu(D)$ with its column module isomorphic to M. So for some $f(D) \in R$ with $\mu(D)R \subset f(D)R$, $\sigma^{-1}(M^k) = \overline{f(D)}\overline{R}$, where $\overline{R} = R/R\mu(D)$. Clearly $f(D)$ is regular with its bound $\lambda(D)$ a factor of $\mu(D)$. Then by (iii)

$$M = f(D)\Omega_k(\mu(D)I_k) \in L_k(F).$$

This proves the proposition. ∎

It is now immediate from Proposition 2.4(iv) that $L_k(F)$ is closed under finite sums and intersections. Let $\Omega_k(f_i(D)) \in L_k(F)$, $1 \leqslant i \leqslant r$. Let $\lambda_i(D)$ be the bound of $f_i(D)$ and $\lambda(D)$ be the lcm of the $\lambda_i(D)$'s. By the above proposition and the isomorphism σ in (2.2) we get

$$\sum_{i=1}^{r} \Omega_k(f_i(D)) = \sum_{i=1}^{r} f_i^*(D)\frac{\lambda(D)}{\lambda_i(D)}\Omega_k(\lambda(D)I_k)$$

$$= g(D)\Omega_k(\lambda(D)I_k)$$

$$= \Omega_k\left(\frac{\lambda(D)}{\mu(D)}g^*(D)\right),$$

where

$$g(D)R = \sum_{i=1}^{r} f_i^*(D)\frac{\lambda(D)}{\lambda_i(D)}R \quad \text{and} \quad \mu(D) = \text{bound}(g(D)).$$

This is a formula for finding the sums of members of $L_k(F)$, and a similar formula can be given for intersections. These formulae are analogous to [9, Theorems 8.54, 8.55].

LEMMA 2.5. *Let $f(D) \in R$ be regular and nonunit, and have bound $\lambda(D) = \prod_{i=1}^{m} p_i(D)^{t_i}$, where $p_i(D)$ are distinct monic irreducible polynomials in $F[D]$ and $t_i \geqslant 1$. Let $q_i(D) = \prod_{j \neq i} p_j(D)^{t_j}$. Then*

$$\Omega_k(f(D)) = \oplus \sum_{i=1}^{m} \Omega_k(f_i(D)),$$

where $f_i(D)$ has bound $p_i(D)^{t_i}$ and

$$\Omega_k(f_i(D)) = q_i(D)\Omega_k(f(D)).$$

Proof. Now $\lambda(D)\Omega_k(f(D)) = 0$. As $R\Omega_k(f(D)) = \Omega_k(\lambda(D)I_k)$ by Theorem 2.3, we get that the annihilator of $\Omega_k(f(D))$ in $F[D]$ is $\lambda(D)F[D]$. So the primary decomposition of $\Omega_k(f(D))$ over $F[D]$ gives

$$\Omega(f(D)) = \oplus \sum_{i=1}^{m} q_j(D)\Omega_k(f(D)),$$

and the annihilator of $q_i(D)\Omega_k(f(D))$ in $F[D]$ is $F[D]p_i(D)^{t_i}$. Consequently by using Lemma 2.2 and Proposition 2.4, we get

$$q_i(D)\Omega_k(f(D)) = \Omega_k(f_i(D))$$

for some $f_i(D)$ with bound $p_i(D)^{t_i}$. ∎

For any regular $f(D) \in R$ with bound $\lambda(D)$, as $\Omega_k(f(D)) \subset \Omega_k(\lambda(D)I_k) \approx \Omega_1(\lambda(D))^{k\times 1}$, the fact that each member of $\Omega_1(\lambda(D))$ is ultimately periodic [9, Theorem 8.7], gives that each member of $\Omega_k(f(D))$ is ultimately periodic. For any $S \in \Omega_k(f(D))$, let $\pi(S)$ denote its least period. The following theorem describes a relationship between the periodicities of members of $\Omega_1(\lambda(D))$ and of $\Omega_k(f(D))$.

THEOREM 2.6. *Let $f(D) \in R$ be regular nonunit with bound $\lambda(D)$. For each $S \in \Omega_1(\lambda(D))$, there exists $T \in \Omega_k(f(D))$ such that $\pi(S) = \pi(T)$. Further there exists $T_0 \in \Omega_k(f(D))$ such that $\pi(T)$ divides $\pi(T_0)$ for every $T \in \Omega_k(f(D))$.*

Proof. Let $\{e_{ij} : 1 \leqslant i, j \leqslant k\}$ be the set of matrix units in R. By the isomorphism σ in Lemma 2.2,

$$\Omega_k(\lambda(D)I_k) \approx \bar{R}\bar{e}_{11},$$

where $\bar{R} = R/R\lambda(D)$, as left R-modules. Let $\lambda(D) = \prod_{i=1}^{m} p_i(D)^{t_i}$ with $p_i(D)$ distinct monic irreducible polynomials and $t_i \geqslant 1$. Let $m = 1$. Then $\bar{R}\bar{e}_{11}$ is a uniserial left $\bar{R}$-module of composition length t_1; so is $\Omega_k(\lambda(D)I_k)$. Consider $S' \in \Omega_1(\lambda(D))$. Then $S = [S', 0, 0, \ldots, 0]^T \in \Omega_k(\lambda(D)I_k)$. As $R\Omega_k(f(D)) = \Omega_k(\lambda(D)I_k)$, there exists $S_1 \in \Omega_k(f(D))$ such that $RS_1 = RS$.

Consequently $\pi(S_1) = \pi(S) = \pi(S')$. For $m > 1$, Lemma by 2.5

$$\Omega_k(f(D)) = \oplus \sum_{i=1}^{m} \Omega_k(f_i(D))$$

with each $f_i(D)$ having bound $p_i(D)^{t_i}$.

Now $\Omega_1(\lambda(D)) = \oplus \Sigma_{i=1}^m \Omega_1(p_i(D)^{t_i})$, so $S' = \Sigma_{i=1}^m S_i$, $S_i \in \Omega_1(p_i(D)^{t_i})$. Since $R\Omega_k(f_i(D)) = \Omega_k(p_i(D)^{t_i})$, by the case for $m = 1$, there exists $T_i \in \Omega_k(f_i(D))$ with $\pi(T_i) = \pi(S_i)$. Then $T = \Sigma_i T_i \in \Omega_k(f(D))$ with $\pi(T) = \pi(S')$. Let $S_0 \in \Omega_1(\lambda(D))$ have $\lambda(D)$ as its minimal polynomial, and $T_0 \in \Omega_k(fD))$ be such that $\pi(T_0) = \pi(S_0)$. It is immediate that for any $T \in \Omega_k(f(D))$, $\pi(T) \mid \pi(T_0)$. This proves the theorem. ∎

3. CANONICAL FORM

As in the previous section, $R = (F[D])^{k\times k}$, where F is a Galois field. Let $f(D) \in R$ be regular and nonunit, and have bound $\lambda(D)$. Since, by Lemma (2.5), $\Omega_k(f(D))$ is a direct sum of $\Omega_k(f_i(D))$, with each $f_i(D)$ having its bound $p_i(D)^{t_i}$ for some irreducible polynomial $p_i(D)$, and $t_i \geqslant 1$, we take $\lambda(D) = p(D)^t$ for some monic irreducible polynomial $p(D)$ and $t \geqslant 1$. Let $\{e_{ij} : 1 \leqslant i, j \leqslant k\}$ be a set of matrix units in R. Now $\bar{R} = R/Rp(D)^t$ is a primary uniserial ring. Thus $\bar{R}$ is a QF-ring, and every $\bar{R}$-module is a direct sum of uniserial modules (see Faith [5, Chapter 25]). Consequently, given any left ideal K of $\bar{R}$, one can write

$$\bar{R} = \oplus \sum_{i=1}^{k} \bar{R}\bar{e}_i$$

and

$$K = \oplus \sum_{i=1}^{k} K\bar{e}_i$$

for some orthogonal indecomposable idempotents e_i. Further, K contains no nonzero ideal of $\bar{R}$ if and only if $Ke_i = 0$ for some i. Consequently by

[6, p. 59, Theorem 2] there exists $A \in R$ which is invertible modulo $Rp(D)^t$, such that

$$\overline{RA}\,\overline{f(D)}\,\overline{B} = \oplus \sum_{i=1}^{k} \overline{RA}\,\overline{f(D)}\,\bar{e}_{ii},$$

where $B \in R$ is an inverse of A modulo $Rp(D)^t$. Since bound $(\overline{f(D)}) = \bar{0}$, we have $\overline{RA}\,\overline{f(D)}\,\overline{B}\bar{e}_{ii} = \bar{0}$ for some i. Thus if $RAf(D)B + Rp(D)^t = Rg(D)$, then bound$(g(D)) = p(D)^t$. As $\overline{B} = \overline{A}^{-1}$, by using Lemma 2.1(v) we get

$$g^*(D)R = Af^*(D)R + Rp(D)^t.$$

Thus

$$\begin{aligned}\Omega_k(g(D)) &= g^*(D)\Omega_k\big(p(D)^t I_k\big)\\ &= Af^*(D)\Omega_k\big(p(D)^t I_k\big)\\ &= A\Omega_k(f(D)).\end{aligned}$$

This gives the following.

LEMMA 3.1. *Let $f(D) \in R$ be regular with bound $p(D)^t$ for some monic irreducible polynomial $p(D)$ and $t \geqslant 1$. Then there exists $A \in R$, which is invertible modulo $Rp(D)^t$, and $g(D) \in R$ with bound $p(D)^t$ such that*

$$\overline{RA}\,\overline{f(D)}\,\overline{B} = \overline{R}\,\overline{g(D)} = \oplus \sum_{i=1}^{k} \overline{R}\,\overline{g(D)}\,e_{ii},$$

and

$$\Omega_k(g(D)) = A\Omega_k(f(D));$$

here $\overline{B}$ is the inverse of $\overline{A}$.

We now prove the main theorem.

THEOREM 3.2. *Let $f(D) \in R$ be regular nonunit with bound $p(D)^t$ for some irreducible polynomial $p(D)$ and $t \geqslant 1$. Then there exists $A \in R$ invertible modulo $Rp(D)^t$ such that*

$$A\Omega_k(f(D)) = \left[\Omega_1\left(p(D)^{t_1}\right), \Omega_1\left(p(D)^{t_2}\right), \ldots, \Omega_1\left(p(D)^{t_k}\right)\right]^T$$

for some uniquely determined t_i such that $0 \leqslant t_i \leqslant t_{i+1}$ for $i < k$ and $t_k = t$.

Proof. By Lemma 3.1 there exists $A \in R$, invertible modulo $Rp(D)^t$, and $g(D) \in R$ with bound $p(D)^t$, such that in $\bar{R} = R/Rp(D)^t$,

$$\bar{R}\bar{A}\,\overline{f(D)}\,\bar{A}^{-1} = \bar{R}\,\overline{g(D)} = \oplus \sum_{i=1}^{k} \bar{R}\,\overline{g(D)}\,\bar{e}_i,$$

$e_i = e_{ii}$. We can choose A such that the composition length $d(\bar{R}\overline{g(D)}\bar{e}_i) \geqslant d(\bar{R}\overline{g(D)}\bar{e}_{i+1})$. Let $u_i = d(\bar{R}\overline{g(D)}\bar{e}_i)$. Then $u_i \geqslant u_{i+1}$, and as seen above Lemma 3.1, some $\bar{R}\overline{g(D)}e_{ii} = 0$, so that $u_k = 0$. Further, u_i are uniquely determined by the composition lengths of uniserial submodules occurring in any decomposition of $\bar{R}\overline{f(D)}$ as a direct sum of uniserial modules. As $\bar{R}\overline{g(D)}\bar{e}_i$ is uniserial with composition length u_i,

$$\bar{R}\,\overline{g(D)}\,\bar{e}_i = p(D)^{t_i}\bar{R}\bar{e}_i, \qquad t_i = t - u_i.$$

So $\bar{R}\overline{g(D)} = \bar{R}\overline{g_1(D)}$, where

$$g_1(D) = \operatorname{diag}\left(p(D)^{t_1}, p(D)^{t_2}, \ldots, p(D)^{t_k}\right)$$

with $t_i \leqslant t_{i+1}$ for $i < k$ and $t_k = t$. Then

$$g_1^*(D) = \operatorname{diag}\left(p(D)^{t-t_1}, p(D)^{t-t_2}, \ldots, p(D)^{t-t_k}\right).$$

Hence by Lemma 3.1

$$A\Omega_k(f(D)) = \Omega_k(g_1(D)) = g_1^*(D)\Omega_k\big(p(D)^t I_k\big)$$

$$= \big[\Omega_1\big(p(D)^{t_1}\big), \Omega_1\big(p(D)^{t_2}\big), \ldots, \Omega_1\big(p(D)^{t_k}\big)\big]^T.$$

Let $A' \in R$ be an inverse of A modulo $Rp(D)^t$. Then

$$\Omega_k(f(D)) = A'\big[\Omega_1\big(p(D)^{t_1}\big), \Omega_1\big(p(D)^{t_2}\big), \ldots, \Omega_1\big(p(D)^{t_k}\big)\big]^T.$$

So by Lemmas 1.1 and 2.2(ii) we get

$$\overline{f^*(D)}\,\overline{R} \approx A_1 \oplus A_2 \oplus \cdots \oplus A_k,$$

where A_i is a uniserial right $\overline{R}$-module of composition length t_i. Consequently t_i are uniquely determined by $\overline{f^*(D)R}$. ∎

In [13] an algorithm has been given to find a basis of $\Omega_1(\lambda(D))$ for any $\lambda(D) \in F[D]$. Using this algorithm, the above theorem can help to write down a basis of $\Omega_k(f(D))$. The distribution of sequences of different periodicities in $\Omega_1(\lambda(D))$ is well known. The above theorem, together with the known results on distribution in $\Omega_1(\lambda(D))$, can be used to give the distribution of sequences of different periodicities in $\Omega_k(f(D))$. For a fixed t and a fixed k, the number of canonical forms given by the above theorem is

$$\sum_i \binom{k-1}{i}\binom{t}{i}, \qquad 0 \leqslant i \leqslant \min(k-1, t).$$

We end this paper with an elementary example of the concepts and results given in it.

EXAMPLE 3.3. Let

$$F = \{0,1,2\}, \qquad F(D) = \begin{bmatrix} 1 & D \\ D & 1 \end{bmatrix}.$$

Then

$$f^*(D)=\begin{bmatrix} -1 & D \\ D & -1 \end{bmatrix} \quad \text{and} \quad \text{bound}(f(D))=D^2-1=(D-1)(D+1).$$

Now $\Omega_1(D^2-1)$ is the set of all sequences over F of the type $S_{(\alpha,\beta)}=(s_n)$, $s_{2n}=\alpha$, $s_{2n+1}=\beta$. So $\Omega_2(f(D))=f^*(D)\Omega_2((D^2-1)I_2)$ is the set of sequences over $F^{2\times 1}$ of the form (ω_n) such that for some $\alpha,\beta\in F$

$$\omega_{2n}=\begin{bmatrix} \alpha \\ -\beta \end{bmatrix}, \qquad \omega_{2n+1}=\begin{bmatrix} \beta \\ -\alpha \end{bmatrix}.$$

Here $p_1(D)=D-1$, $p_2(D)=D+1$, $q_1(D)=D+1$, $q_2(D)=D-1$. Further, $q_1(D)\Omega_2(f(D))$ is the set of sequences of the form (v_n) such that for some $\alpha\in F$,

$$v_n=\begin{bmatrix} \alpha \\ -\alpha \end{bmatrix}.$$

Now $q_1(D)f^*(D)R+(D^2-1)R=g_1(D)R$, where

$$g_1(D)=\begin{bmatrix} D+1 & 0 \\ -D^2-D & 1-D^2 \end{bmatrix}, \qquad g_1^*(D)=\begin{bmatrix} D-1 & 0 \\ -D & -1 \end{bmatrix}.$$

Then

$$q_1(D)\Omega_2(f(D))=\Omega_2(g_1^*(D)).$$

Similarly $q_2(D)\Omega_2(f(D))$ consists of sequences of the form (v_n) such that for some $\alpha\in F$,

$$v_{2n}=\begin{pmatrix} \alpha \\ -\alpha \end{pmatrix}=-v_{2n+1},$$

and it equals $\Omega_2(f_2(D))$, where

$$f_2(D)=\begin{bmatrix} D+1 & 0 \\ -D & -1 \end{bmatrix}.$$

The author is extremely thankful to the referee for his various suggestions.

REFERENCES

1 D. E. Daykin, On linear sequences over finite fields, *Amer. Math. Monthly* 70:637–642 (1963).
2 D. J. DeCarli, A generalized Fibonacci sequence over any arbitrary ring, *Fibonacci Quart.* 8:182–184 (1970).
3 H. J. A. Duparc, Periodicity properties of recurring sequences I, *Indag. Math.* 16:331–342 (1954).
4 H. J. A. Duparc, Periodicity properties of recurring sequences II, *Indag Math.* 16:473–485 (1954).
5 C. Faith, *Algebra II, Ring Theory*, Grundlehren Math. Wiss. 191, Springer-Verlag, 1976.
6 N. Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloq. Publ. 27, 1964.
7 A. V. Jategaonker, *Left Principal Ideal Rings*, Lecture Notes in Math. 123, Springer-Verlag, 1970.
8 L. Levy, Torsionfree and divisible modules over non-integral domains, *Canad. J. Math.* 15:132–151 (1963).
9 R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, 1983.
10 M. B. Nathanson, Difference operators and periodic sequences over finite modules, *Acta Math. Hungar.* 29:219–224 (1976).
11 D. W. Robinson, The rank and period of linear recurrent sequences over a ring, *Fibonacci Quart.* 14:210–214 (1976).
12 C. Ronse, *Feedback Shift Registers*, Lecture Notes in Comput. Sci. 169, Springer-Verlag, 1984.
13 S. Singh, A note on linear recurring sequences, *Linear Algebra Appl.* 104:97–101 (1988).
14 M. Wards, The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.* 35:600–628 (1932).

Received 21 June 1988; final manuscript accepted 9 February 1989